

Serial No.: 09/929,094

REMARKS

Applicants respectfully request reconsideration of this Patent Application, particularly in view of the above Amendment and the following remarks. No additional fee is required for this Amendment as the number of independent claims has not changed, and the total number of claims has not changed.

Request for Telephone Interview

Applicants believe a telephone interview before the Examiner continues consideration would beneficially expedite prosecution. Therefore, Applicants kindly request the Examiner to contact the undersigned at (847) 490-1400 to schedule a telephone interview, to discuss the merits of this Patent Application.

Amendment to the Claims

Applicants have made many amendments to the claims in attempts to clarify limitations and issues. The Examiner is free to contact Applicants' undersigned attorney for a clean copy of the claims if it would be helpful. Support for the Amendment can be found throughout Applicants' Specification, and specific exemplary portions are noted below for convenience. No new matter has been added to the claims by this Amendment, and Applicants have followed the guidelines of MPEP 2163.02 for portions of this Amendment.

Applicants have added new independent Claim 28 and have amended independent Claim 1 to depend from new Claim 28. Claim 15 has been canceled and replaced with new Claim 29, which also depends from Claim 28. Support for new Claim 28 can be found at page 5, last paragraph, through page 9, second paragraph. Claims 2-9 and 17-21 have been amended in view of new Claims 28 and 29 and

Serial No.: 09/929,094

amended Claim 1, respectively, to correct dependencies, provide proper antecedent bases, and to otherwise clarify the claimed invention. Claim 16 has been canceled without prejudice.

Claim 10 has been amended to recite the monitoring of both a content of digital data gathering results and a further content of further digital data gathering results. Claims 11-13 have been amended in view of amended Claim 10, to correct dependencies, provide proper antecedent bases, and to otherwise clarify the claimed invention. Support can also be found at page 5, last paragraph, through page 9, second paragraph.

Claim 14 has been amended for clarity under authority from MPEP 2163.02. Support can also be found at page 8, last paragraph, through page 9, second paragraph, and page 18, last paragraph.

Claim 22 has been amended to clarify the claimed invention.

Claim 23 has been amended to recite that the clustering is based upon content. Support can be found at page 6, first and second paragraphs.

Claims 24 -26 have been amended for clarity.

Serial No.: 09/929,094

Claim Rejections - 35 U.S.C. §103

Applicants again request the Examiner to contact the undersigned before further consideration, as Applicants believe a telephone interview would beneficially expedite prosecution.

The rejection of Claims 1, 2, 7, and 14 under 35 U.S.C. §103(a) as being unpatentable over Lermuzeaux et al., U.S. Patent 5,621,889, in view of Oblinger, U.S. Publication 2002/0107852, is respectfully traversed.

Claims 1, 2, and 7 now depend from Claim 28. Claim 28 recites monitoring content of queries and/or results obtained by the user. Applicants' claimed invention detects misuse based upon content of the use, not merely analyzing characteristics of system use, like the Lermuzeaux et al. Patent. The differentiation between "content" detection and "system" detection is important in understanding the differences between Applicants' claimed invention and the cited prior art references.

System detection, which is available in the prior art, such as the Lermuzeaux et al. Patent, is based upon system usage characteristics. For example, if a given user normally types at speeds of 30 words per minute, and now is typing at 95 words per minute, that is unlikely the same user. Furthermore, if a user always issues "ls-la" (Unix list command with several options) and now always uses only "ls," it might indicate strange behavior. Similarly, if all file names in the past were long and descriptive in nature and now the user is naming files simply "a," "b," "c," and so on, this is also strange. None of these system detection measures are based on anything to do with the CONTENT of the actual files being accessed. Content detection is based upon the content of the queries and results of the user.

The Lermuzeaux et al. Patent is clearly teaching system detection. At Col. 2, lines 9-14, the Lermuzeaux et al. Patent says the facility of the invention

Serial No.: 09/929,094

makes use of “streams of surveillance data relating to the operation of the computer installations and in particular to the actions of users of said installations.” This passage clearly indicates to one skilled in the art that the disclosure is system oriented, and says nothing about content detection. Reading Applicants’ content detection into this passage is an application of improper hindsight.

Furthermore, the Lermuzeaux et al. Patent discloses at Col. 6, lines 27-29, that the monitor transmits “audit data.” The term “audit data” appears throughout the patent. “Audit data” is known to one skilled in the art to be related to system detection. The Lermuzeaux et al. Patent, alone or in combination with the Oblinger Patent, does not teach or suggest Applicants’ claimed invention. The Oblinger Patent evidences data clustering exists, but the only suggestion for misuse detection based upon content, and content clusters, comes from Applicants’ disclosure. Thus this rejection is made using hindsight that is improper.

Claim 14 as been amended to recite “employment information” instead of workplace characteristics. The prior art does not teach or suggest constructing a structured data profile for a user based upon employment information, e.g., vacation status, job description, etc. As discussed above, the prior art relies on system information, not employment information of the user, in detection intrusion. Amended Claim 14 overcomes the current rejection.

Favorable reconsideration and withdrawal of rejections based upon the Lermuzeaux et al. Patent are respectfully requested.

The rejection of Claims 3-6 and 9 under 35 U.S.C. §103(a) as being unpatentable over Lermuzeaux et al., U.S. Patent 5,621,889, in view of Oblinger, U.S. Publication 2002/0107852, and further in view of Lane et al., is respectfully traversed.

Serial No.: 09/929,094

Claims 3-6 and 9, ultimately depend from new Claim 28, and are patentable for at least the same reasons presented above. The Lane et al. Article, discussed more below, also teaches system detection.

The rejection of Claim 8 under 35 U.S.C. §103(a) as being unpatentable over Lermuzeaux et al., U.S. Patent 5,621,889, in view of Oblinger, U.S. Publication 2002/0107852, and further in view of Parker et al., U.S. Patent No. 5,909,589, is respectfully traversed. Claim 8 also ultimately depends from new Claim 28, and is patentable for at least the same reasons presented above. The Parker et al. Patent, discussed more below, also teaches system detection.

The rejection of Claims 10-12 under 35 U.S.C. §103(a) as being unpatentable over Parker et al., U.S. Patent No. 5,909,589, in view of Lane et al., is respectfully traversed. Claim 10 has been amended to clarify that the content of the results is monitored and used to identify misuse. Claims 11 and 12 depend from amended Claim 10.

The Parker et al. Patent teaches a method of identity verification of a student during computer-based training sessions. The Parker et al. Patent is also a system detection method, and not related to Applicants' content-based detection method. The Parker et al. Patent discloses verifying identity by system information, such as typing patterns, mouse click patterns, and/or misspelling patterns (Col. 2, lines 41-46). The verification is according to system-based habits, not the content of any search results. The Office Action cites to Col. 11, lines 16-44, for teaching comparing words or phrases of the digital data gathering results to the user lexicon ... This citation is incorrect, as this portion of the Parker et al. Patent is talking about

Serial No.: 09/929,094

“systems environment” (line 15). Nowhere in this passage is content comparison discussed.

The Office Action cites the Lane et al. Article, without reference to any particular passage, for teaching “that based upon user’s past queries, a dictionary is created with the most-likely commands/terms used historically by that user.” The Lane et al. Article is also teaching a system, not content, detection. For example, the abstract, page 296, first paragraph, and page 298, second paragraph, talk about user behavior. “Behavior” is not content of search results, as in Applicant’s claimed invention. The Office Action, at page 4, also emphasizes “network packet traffic” at page 296, lines 1-7, of the Lane et al. Article, which of course is a system property, and not relevant to content of search results.

Applicants’ Amendment clarifies that the Lane et al. Article is not relevant to Applicants’ claimed invention. Favorable reconsideration and withdrawal of this rejection are respectfully requested.

The rejection of Claim 13 under 35 U.S.C. §103(a) as being unpatentable over Parker et al., U.S. Patent No. 5,909,589, in view of Lane et al., and further in view of Lermuzeaux et al., U.S. Patent 5,621,889, is respectfully traversed. Claim 13 depends from Claim 10, and is patentable for at least the same reasons presented above.

The rejection of Claims 15-21 under 35 U.S.C. §103(a) as being unpatentable over Lermuzeaux et al., U.S. Patent 5,621,889, in view of Oblinger, U.S. Publication 2002/0107852, and further in view of Lane et al., is respectfully traversed.

Serial No.: 09/929,094

Claims 15-16 have been canceled, and Claims 17-21 now ultimately depend from new Claim 28. The above remarks regarding why these prior art references are irrelevant as system detection methods, and not content-based misuse detection methods as in Applicants' claimed invention, is incorporated herein and won't be restated for brevity.

The rejection of Claim 22 under 35 U.S.C. §103(a) as being unpatentable over Herz et al., U.S. Patent 5,835,087, in view of Lane et al., is respectfully traversed.

The Herz et al. Patent is cited as evidence that clustering exists. The Herz et al. Patent teaches forming clusters that are of interest to a person, and has no relevance to using clusters to detect unauthorized misuse, as in Applicants' claimed invention. The Lane et al. Article is cited for using the clusters to determine whether a misuse has occurred. However, the Lane et al. Article, as discussed above, is based upon system detection, not content detection. Again, the Office Action insufficiently, and incorrectly, makes claims about the Lane et al. article establishing a dictionary based upon past queries for detecting anomalies without citing to particular passages in the Lane et al. Article.

Content-based clusters of the Herz et al. Patent are irrelevant to the system detection method of the Lane et al. Article. The only suggestion to use content clusters to identify misuse comes from Applicants' disclosure. Without the benefit of Applicants' disclosure, one skilled in the art would have not motivation to combine the teachings of these unrelated prior art references.

Favorable reconsideration and withdrawal of this rejection are respectfully requested.

Serial No.: 09/929,094

The rejection of Claim 23 under 35 U.S.C. §103(a) as being unpatentable over Lane et al., in view of Zhang et al., U.S. Patent 5,832,182, is respectfully traversed. Claim 23 has been amended to recite that the categorizing is based upon content. As discussed above, the Lane et al. Article teaches a system detection method, and not a content-based misuse detection method as in Applicants' claimed invention.

Applicants have reviewed Sections 2.2.1 - 2.2.4 of the Lane et al. Article noted in the Office Action. Applicants do not understand where in these passages the Examiner finds the teachings alleged in the second paragraph of section IX on page 23. For example, the Office Action cites Section 2.2.1 for teaching retrieving documents in response to user queries. Section 2.2.1 is talking about UNIX shell command data in the system history data. Section 2.2.1 does not discuss anything remotely similar to retrieving documents in response to user queries.

The Zhang et al. Patent discloses data clustering for large databases. Combining the Zhang et al. Patent with the Lane et al. Article does not provide or suggest Applicants' claimed invention.

Favorable reconsideration and withdrawal of this rejection are respectfully requested.

The rejection of Claims 24 and 25 under 35 U.S.C. §103(a) as being unpatentable over Lane et al., in view of Herz et al., U.S. Patent 5,835,087, is respectfully traversed.

As discussed above, the Lane et al. Article teaches a system detection method, and not a content-based misuse detection method as in Applicants' claimed invention.

Serial No.: 09/929,094

Applicants have reviewed Sections 2.2.1 - 2.2.4 of the Lane et al. Article noted in the Office Action. Applicants do not understand where in these passages the Examiner finds the teachings alleged in the second paragraph of section X on page 24. For example, the Office Action cites Section 2.2.1 for teaching identifying top weighted terms from documents retrieved by the user and storing the top weighted terms in a user-specific lexicon. Section 2.2.1 is talking about UNIX shell command data in the system history data. These commands are not reasonably considered top weighted terms from retrieved documents. These commands are typed system commands that originate from the user, and not from a search of an information retrieval system. Section 2.2.1 does not discuss anything remotely similar to identifying top weighted terms from documents retrieved by the user.

The Herz et al. Patent teaches forming clusters that are of interest to a person, and has no relevance to using clusters to detect unauthorized misuse, as in Applicants' claimed invention.

Favorable reconsideration and withdrawal of this rejection are respectfully requested.

The rejection of Claim 26 under 35 U.S.C. §103(a) as being unpatentable over Oblinger, U.S. Publication 2002/0107852, in view of Lane et al. is respectfully traversed.

The Oblinger Patent evidences data clustering exists. The Oblinger Patent discloses, at paragraphs [0049] and [0060], identifying search attributes/needs of a particular user. The system over time learns to predict the user needs/behavior and suggests new user contexts for the system (Paragraph [0049]). Nothing in the Oblinger Patent, particularly the passages noted by the Examiner, indicates the

Serial No.: 09/929,094

invention is at all pertinent to misuse detection. The combination is based upon the allegation that the Lane et al. Article teaches comparing UNIX command data to data histories for comparison.

The rejection attempts to provide Applicants' invention by pairing a content clustering patent with a system-oriented detection method. There is simply no reason outside of Applicants' disclosure to combine the teachings of these two unrelated prior art references. Why would one skilled in the art modify the method of the Oblinger Patent to determine discrepancies between past and present "commands/queries" and send an alarm when this has nothing to do with the purpose of the Oblinger Patent. The Oblinger Patent is not an intrusion detection method.

The Office Action's purported motivation for combining these references is nonsensical. The Office Action states at page 26:

This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

Whether the above statement is accurate or not, it has nothing to do with the subject matter of the Oblinger Patent and is not a valid motivation to combine. The Lane et al. Article is the only one of these two references related to any kind of anomaly detection. Simply put these are not analogous references.

Favorable reconsideration and withdrawal of this rejection are respectfully requested.

Serial No.: 09/929,094

The rejection of Claim 27 under 35 U.S.C. §103(a) as being unpatentable over Oblinger, U.S. Publication 2002/0107852, in view of Herz, U.S. Patent 5,835,087, and Lane et al. is respectfully traversed.

The above comments for Claim 26 are equally appropriate here and incorporated by reference. Neither the Herz et al. Patent nor the Oblinger Patent is an intrusion detection method. Why would one skilled in the art apply teachings of the Lane et al. Article with these two documents when they are directed to very different purposes.

The Office Action's purported motivation for combining these references is again nonsensical. The Office Action states at page 27:

This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Lane et al. suggests that similarities in the user's current behavior when typing commands/queries and the accumulated history of the user's behavior are a strong indication of normal usage in section 2.2 (found on pages 300-301).

Whether the above statement is accurate or not, it has nothing to do with the subject matter of either of the Oblinger or Herz Patents and is not a valid motivation to combine. The Lane et al. Article is the only one of these references related to any kind of anomaly detection. Simply put these are not analogous references with no reason to combine.

Favorable reconsideration and withdrawal of this rejection are respectfully requested.


Serial No.: 09/929,094

Conclusion

Applicants intend to be fully responsive to the final Office Action. If the Examiner detects any issue which the Examiner believes Applicants have not resolved in this response, Applicants' undersigned attorney again requests a telephone interview with the Examiner.

Applicants sincerely believe that this Patent Application is now in condition for allowance and, thus, respectfully request early allowance.

Respectfully submitted,



Mark D. Swanson
Regis. No. 48,498

Pauley Petersen & Erickson
2800 West Higgins Road
Suite 365
Hoffman Estates, Illinois 60195
(847) 490-1400
FAX (847) 490-1403